Weaponizing Corporate Intel

This Time, It's Personal!

Beau Bullock (@dafthack)
Mike Felch (@ustayready)

Overview

- This is an OSINT / Recon / Pseudo-attack talk! We are going to cover stuff you might already know as well as some brand new techniques!

- Going from zero knowledge of an organization to stalker status
- External resource targeting (w/ less attribution)
- Internal employee targeting (at a personal level)
- Advanced password stuffing attacks
- Out-of-Band Phishing

About Us

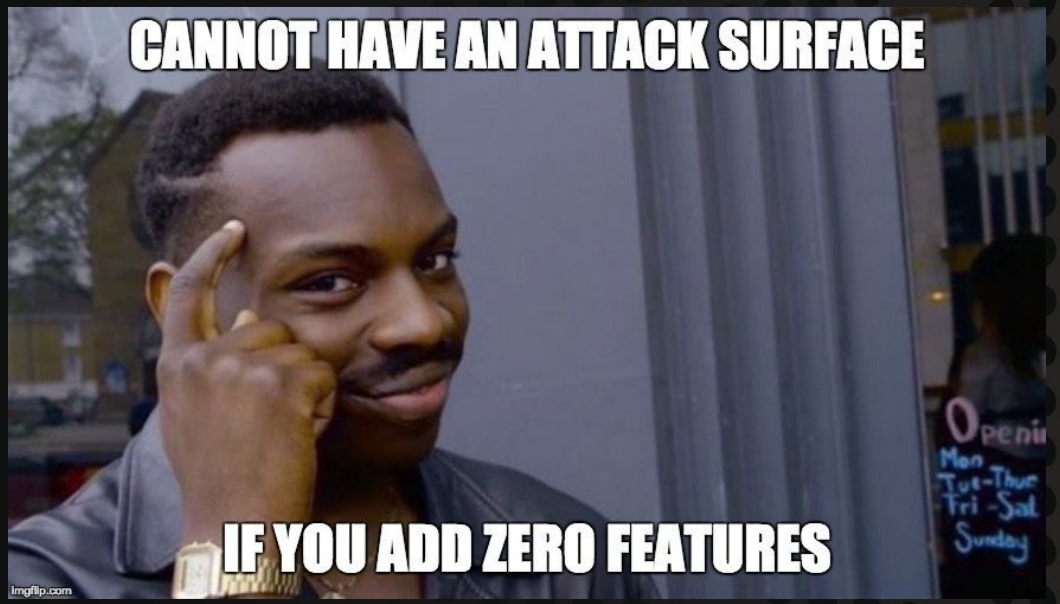
- Mike Felch - @ustayready
  - Pentest / Red team at BHIS
  - Involved w/ OWASP Orlando
  - Host of Tradecraft Security Weekly
  - Host of CoinSec Podcast
- Beau Bullock - @dafthack
  - Pentest / Red team at BHIS
  - Host of Tradecraft Security Weekly
  - Host of CoinSec Podcast
  - Avid OWA enthusiast

Attack Surface Recon

External Host Discovery

Scratching the Surface

- 1st step in any operation = Recon
- Build a solid target list
- Gain understanding around technologies used
- Can you determine what is used for:
  - Remote access
  - Email access
  - Security products

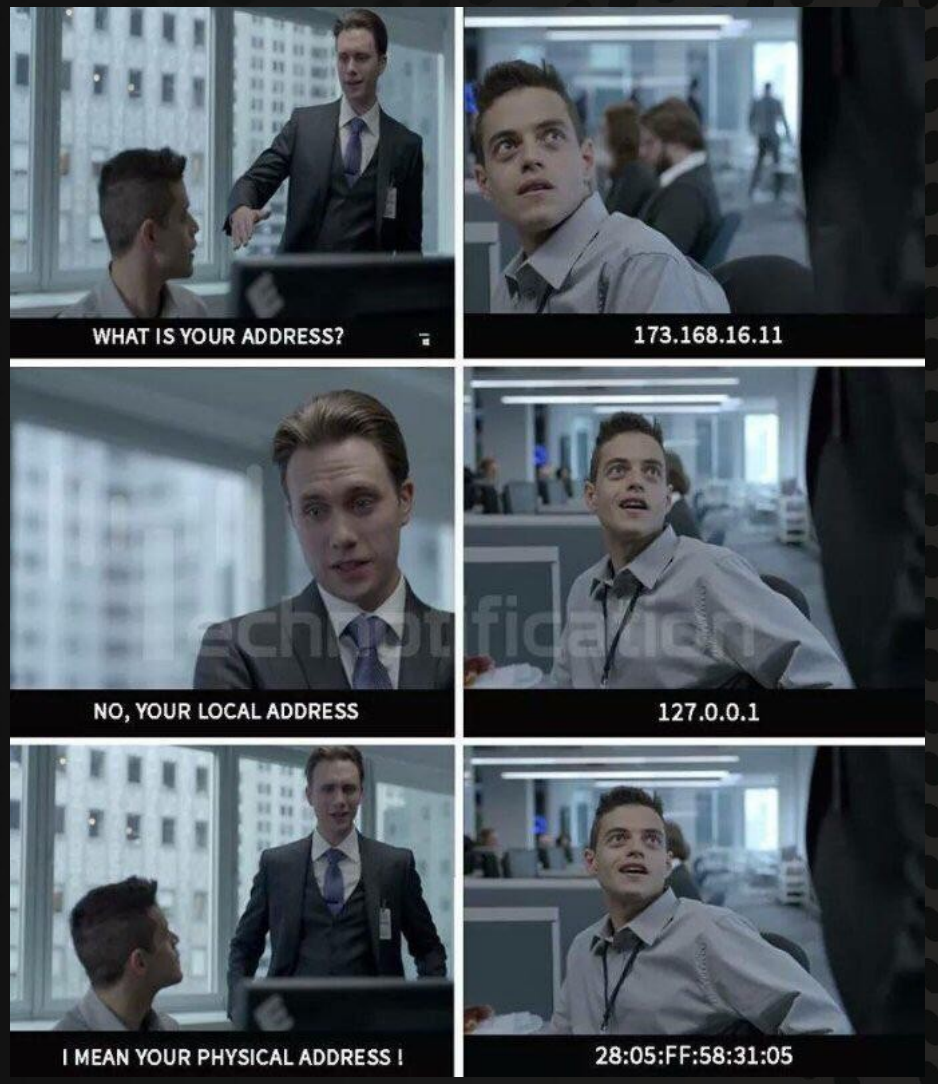


TLDs and Subdomains

- Utilize search engines and “dorking”
  - Google
  - Bing
  - Baidu
  - DuckDuckGo
- Recon-NG Modules
  - recon/domains-hosts/bing_domain_api
  - recon/domains-hosts/google_site_web

Netblocks

- ASN / Netblock Discovery
  - https://bgp.he.net
  - https://mxtoolbox.com/arin.aspx
- Regional Internet Registry Search
  - https://whois.arin.net
  - Also AFRNIC, APNIC, LACNIC, and RIPE
- Recon-NG Module
  - recon/companies-multi/whois_miner



TLDs and Subdomains

- Subdomain Discovery
  - shodan.io - recon/domains-hosts/shodan_hostname
  - censys.io - recon/netblocks-ports/censysio
  - dnsdumpster.com
  - hackertarget.com - recon/domains-hosts/hackertarget
  - threatcrowd.org - recon/domains-hosts/threatcrowd
  - Subdomain bruteforcing - recon/domains-hosts/brute_hosts

TLDs and Subdomains

- Additional TLD and Subdomain Discovery
  - crt.sh
  - Search netblocks on shodan.io
- Rinse and repeat with new TLDs and netblocks

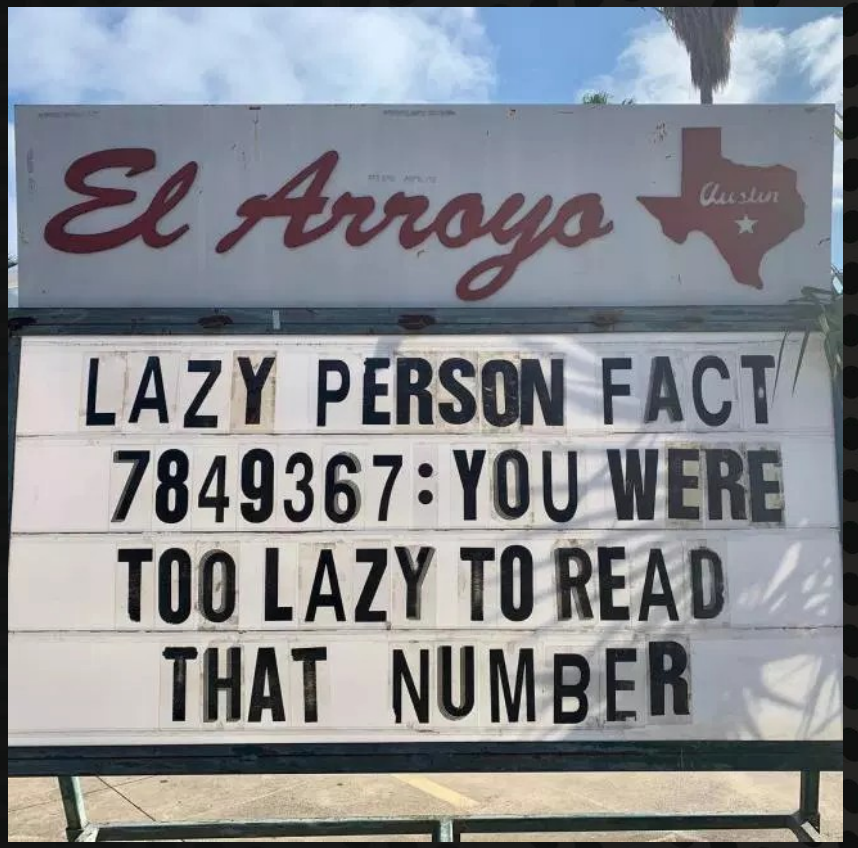
- Recon-NG Modules
  - recon/domains-hosts/certificate_transparency
  - recon/netblocks-hosts/shodan_net

Cloud Services

- Microsoft Services
  - O365 - Go to outlook.office365.com and try authenticating with test@targetdomainname.com
  - SharePoint - Check companyname.sharepoint.com
  - Find Skype4Business - lyncdiscover.targetdomaindomain.com

Cloud Services

- Google
  - Try authenticating with a valid company email address at Gmail
- Box.com
  - Try https://companyname.account.box.com
- Amazon AWS
  - Look to see where web resources are being loaded. Potentially pointing to S3 buckets.



Portal to Pwnage

Discovering Login Forms and Other Interesting Files

@BHInfoSecurity

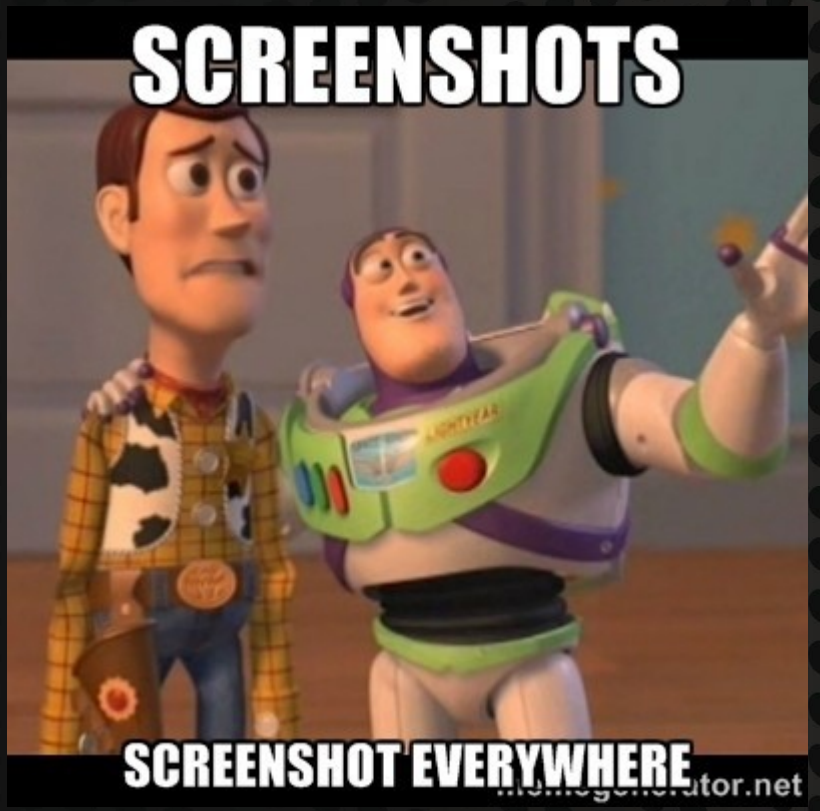
Active Portal Discovery

- Actively scan to locate web services
- Portscan domain list on common web ports (80, 443, 2381, 8080, 8443, 10000, etc.)
- Could manually review results navigating to each service with a browser…

- Or…

Active Portal Discovery

- Screenshot webapps with EyeWitness by Chris Truncer
  - https://github.com/FortyNorthSecurity/EyeWitness
- Quickly analyze many portals
- Groups common web responses
- I like to make a secondary list of interesting web servers as I go through the results



Interesting File/Dir Discovery

- Directory/File bruteforcing at scale with **Brute-Fruit**
  - Module in Find-Fruit PowerShell script
  - https://github.com/rvrsh3ll/Misc-Powershell-Scripts/blob/master/Find-Fruit.ps1
- Use file list + web server list
- Discover interesting portals and pages

BruteFruit Demo

Remotely Gathering Internal Domain Information

"The more you know!"

@BHInfoSecurity

Info Disclosure FTW

- Information disclosure vulns = **Low**
  …in most cases
- But they are **Critical** to an attackers methodology
- In order to successfully perform password attacks we need to be confident about two things:
  - Username format
  - Probability most users can authenticate

Discovering Username Schema

- User Enumeration Vulns
- Some applications will let you know a username is valid or not on login
- Microsoft OWA response time vuln
  - MailSniper Invoke-UsernameHarvestOWA module

Discovering Username Schema

- Metadata attached to files (PDF, DOCX, XLSX, etc.)
- PowerMeta – Search for publicly available files hosted by a company, then extract metadata from each file
  - https://github.com/dafthack/PowerMeta

```
PS C:\> Invoke-PowerMeta -TargetDomain "[redacted].com"

[*] Searching Google for 'site:[redacted].com filetype:
pdf'
[*] Now Analyzing page 1 of Google search results (100
 results per page)
[*] Searching Bing for 'site:[redacted].com filetype:pd
f'
[*] Now Analyzing page 1 of Bing search results (30 re
sults per page)
```

```
[*] Extracted 'Author' and 'Creator' metadata

"C:/Users/beau/Desktop/PowerMeta/2017-04-05-113740/Artifacts
"[redacted]"
%2[redacted]df"
%2[redacted]ion
Adobe InDesign CS3 (5.0.2)
AutoBVT
c[redacted]d
[redacted]
Dennis [redacted]
k[redacted]r
Microsoft┬« Word 2010 Subscription
Microsoft┬« Word 2013
[redacted]
```

Possible Usernames

Full Name

One Problem

- Servers can detect IP activity
- Servers will block requests
- How can we avoid detection?
- Would be nice to rotate IPs!
- SOCKS? ProxyCannon? CredKing?
- All have limits or are expensive ☹
- Hmmm…

Introducing FireProx

https://github.com/ustayready/fireprox

FireProx

- Rotates IP with every request! ☺
- Leverages AWS API Gateway
- HTTP Pass-through proxy
- Point FireProx at URL and go!
- Scrape, Spray, or Crawl
- Avoid CAPTCHA and WAF restrictions
- ~~Downside: X-Forwarded-For sent ☹~~
  - Custom X-My-X-Forwarded-For (thanks Fred Reimer)

FireProx Demo

So far…

- We've found great hosts and portals
- We've identified running services
- We've got target servers in sight

- … we just need to find employees
- … but can we change our attacks?

Introducing Social Trust Attacks

@BHInfoSecurity

Social Trust Attacks

- Breaching organizations w/ employee personal data
- Employees aren't trained on personalized attacks ☹
- New type of spear-phishing/SE
- New type of password attacks
- What if…
  - We get personal information of employees?
  - We get personal relationships of employees?
  - We get personal emails of employees?

Discover Employees

- Nothing new here… except more data
- LinkedIn scraping company employees
- Profile URLs from Google/Bing/etc
- site:linkedin.com/in/ “company name”
- Grab:
  - first name & last name
  - **city** & **state**

Email Formatting

- Hunter.io is great for learning format
- RocketReach.co is good too
- Combine names into company format
- EmailAddressMangler on GitHub

- … now we have **company email**!

Need moar data!@#

- Can we get PII/personal emails of employees?
- Can we learn their relationships?
- People Data Brokers give us everything!
  - They buy, sell, trade, and give our data at scale
- They collect and aggregate our public data
  - i.e. https://www.truepeoplesearch.com/
- Query people sites using name & location
  - Now we have PII, personal emails, & relationships

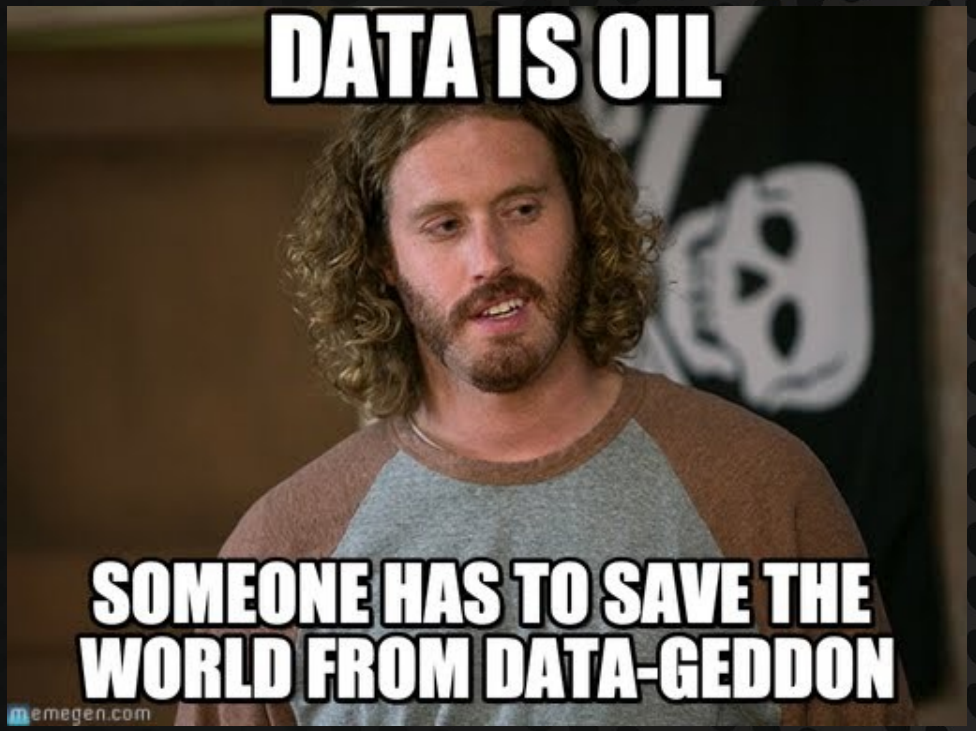
People Sites.. Opt Out (or abuse)!

- **http://www.peoplefinders.com/**
- http://www.whitepages.com/
- http://www.spokeo.com/
- http://www.instantcheckmate.com/
- http://www.intelius.com/
- http://www.peoplesmart.com/
- http://www.mylife.com/
- http://www.peekyou.com/
- http://www.pipl.com/
- http://www.radaris.com/
- http://www.411.com/
- http://www.switchboard.com/
- http://www.peeplo.com/
- http://www.zabasearch.com/
- http://www.anywho.com/
- https://truepeoplesearch.com/
- https://www.fastpeoplesearch.com/

SCREENSHOT THIS ☺

There's way more ☹

- People Data
- Business Data
- Census Data
- Criminal Data
- Debt Data
- Domain Data
- Eviction Data
- Foreclosure Data
- Property Data
- Phone Data
- Work Data
- Marriage Data
- Divorce Data



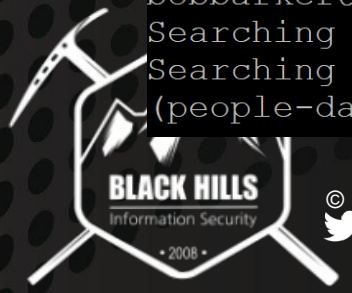
Personal Password Attacks

Personal Passwords Reconciled

- Using personal emails search breach database
  - i.e. Collection #1 - #5
- Get passwords for personal emails
- Reconcile passwords to corporate accounts
- Use personal passwords on corporate portals
- Password reuse problems is a huge problem!

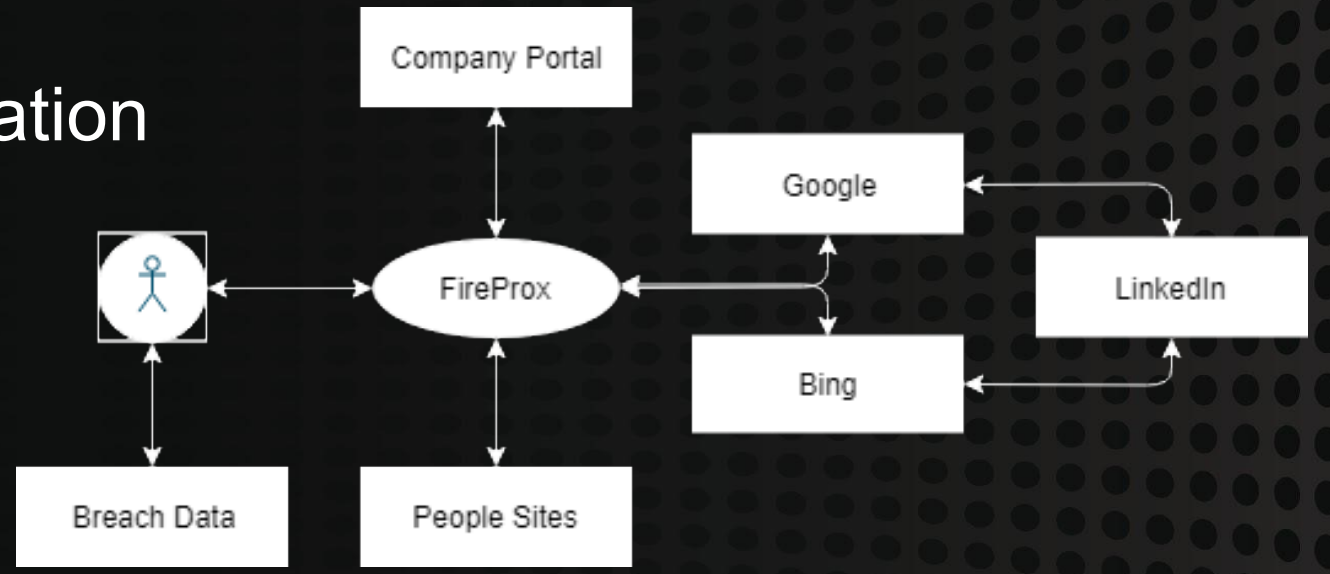
Personal Passwords Reconciled

```
(people-data-parser) ubuntu@ip-10-0-0-197:/projects/people-data-parser$ python breach.py bob barker ventura ca
Searching for bbarker@attbi.com...
Searching for bobbarker13@gmail.com...
bobbarker13@gmail.com
bobbarker13@gmail.com
bobbarker13@gmail.com
bobbarker13@gmail.com
bobbarker13@gmail.com
Searching for bobbarker@gmail.com...
bobbarker@gmail.com:
bobbarker@gmail.com:
bobbarker@gmail.com:
bobbarker@gmail.com:
bobbarker@gmail.com:
bobbarker@gmail.com:
bobbarker@gmail.com:
bobbarker@gmail.com:
bobbarker@gmail.com:
bobbarker@gmail.com:
bobbarker@gmail.com:
Searching for b.barker13@gmail.com...
Searching for bobbarkerpunchespeopleeveryday@yahoo.com...
(people-data-parser) ubuntu@ip-10-0-0-197:/projects/people-data-parser$
```



Attack Path

1. Find portals
2. Scrape employee name/location
3. Format corporate emails
4. Scrape people sites
5. Get personal passwords
6. Reconcile accounts
7. Use personal passwords w/ corporate email on portals



PROFIT!

How to Prepare & Prevent

QUIT RE-USING PASSWORDS!

Social Trust Attacks

@BHInfoSecurity

Social Trust Attacks

- Incorporate personal info in phish
- Leverage known relationships
- Doppel ganging as known contact
- Can come from non-corp domain
- High quality personalization!

Personal Data Prepared

- The amount of data is staggering
- Sites retrieve more data then UI shows
  - All names, aliases, previous names and dates
  - Date of birth / Age
  - Living vs Deceased
  - Current & Previous Addresses w/ Dates & Geo
  - Current & Previous Phones w/ Dates & Telco/Geo
  - Neighbors & Neighborhood Info
  - Email Addresses
  - Relatives & Relative Type w/ DOB
  - Associates w/ DOB
  - Voter Records
  - Employment History

Fast People Search

https://www.fastpeoplesearch.com/marshall-a-mathers-3rd_id_G-6445336243156685362

Search for...

Marshall A Mathers 3RD Age 46

FULL BACKGROUND REPORT AVAILABLE

Current Address

15260 Ventura Blvd, STE 2100
Sherman Oaks, CA 91403-5360

Map

Phone Numbers

(540) 537-1100 - Wireless

(313) 930-1600 - Wireless

(586) 610-6579 - Wireless

Show More...

Email Addresses

marshall.mathers@bellatlantic.net

lil_shady_d12_eminem@hotmail.com

marshall.mathers@hotmail.com

Show More...

Associated Names

Marshall B Mathers 3RD

Marshall B Mathers

Bruce Mathers Marshall

Show More...

https://www.fastpeoplesearch.com/marshall-a-mathers-3rd_id_G-6445336243156685362

Search for...

Previous Addresses

5760 Winkler Mill Rd
Rochester Hills, MI 48306-2153
(12/19/2006 - 7/16/2011)

Map

208 Bellaire Blvd
Lewisville, TX 75067
(7/12/2007 - 9/11/2008)

Map

19766 Westchester Dr
Clinton Township, MI 48038-2387
(12/19/2006 - 12/19/2006)

Map

Show More...

Possible Relatives

Kimberley A Mathers , B Mathers Rd Marshall , Bruce Mathers Marshall 3RD , Debbie R Mathers , Debbie M Mathers , Debbie Mathersbriggs , Debbie R Nelson , Debbie R Nelson ,

Show More...

Possible Associates

Casimer T Sluck , John W Briggs , Jeffrey L Hudock , Kathleen L Sluck , Betti R Schmitt , Bruce S Seckendorf , Christopher John Stapels , Darren Michael Martens ,

Show More...

Possible Businesses

SJH FAMILY HOLDING CORP

15260 Ventura Blvd Ste 2100Sherman Oaks CA 91403

Exaggerated… Personalized Phish

Hey <first name>! How have you been? It's <associate first name> from <previous city>. I haven't talked to you since you lived over on <previous street name>! I tried calling <previous phone number> but it said it was disconnected. Hope you don't mind me emailing you at work. I was trying to reach out to see if you heard the news about <mutual associate name>? I couldn't believe it when I heard the news and then I read the news article <phishing link> and was convinced it was true. Anyhow, I hope you are well. Feel free to email me when you get some time.

- <associate first name> <associate last name>

How to Prepare & Prevent

- Reduce your digital footprint
- Watch for personal emails @ work
- Start opting out everywhere
  - Vermont data brokers search
  - https://www.vtsosonline.com/online/BusinessInquire/
- Become an EU resident!
  - Estonia eResident program
  - https://e-resident.gov.ee/
  - GDPR Erasure clauses

Questions

- Black Hills Information Security
  - http://www.blackhillsinfosec.com
  - @BHInfoSecurity
- Beau Bullock @dafthack
- Mike Felch @ustayready

Mike's journey reducing data (leaving Google services)

- https://www.blackhillsinfosec.com/how-to-purge-google-and-start-over-part-1/
- https://www.blackhillsinfosec.com/how-to-purge-google-and-start-over-part-2/